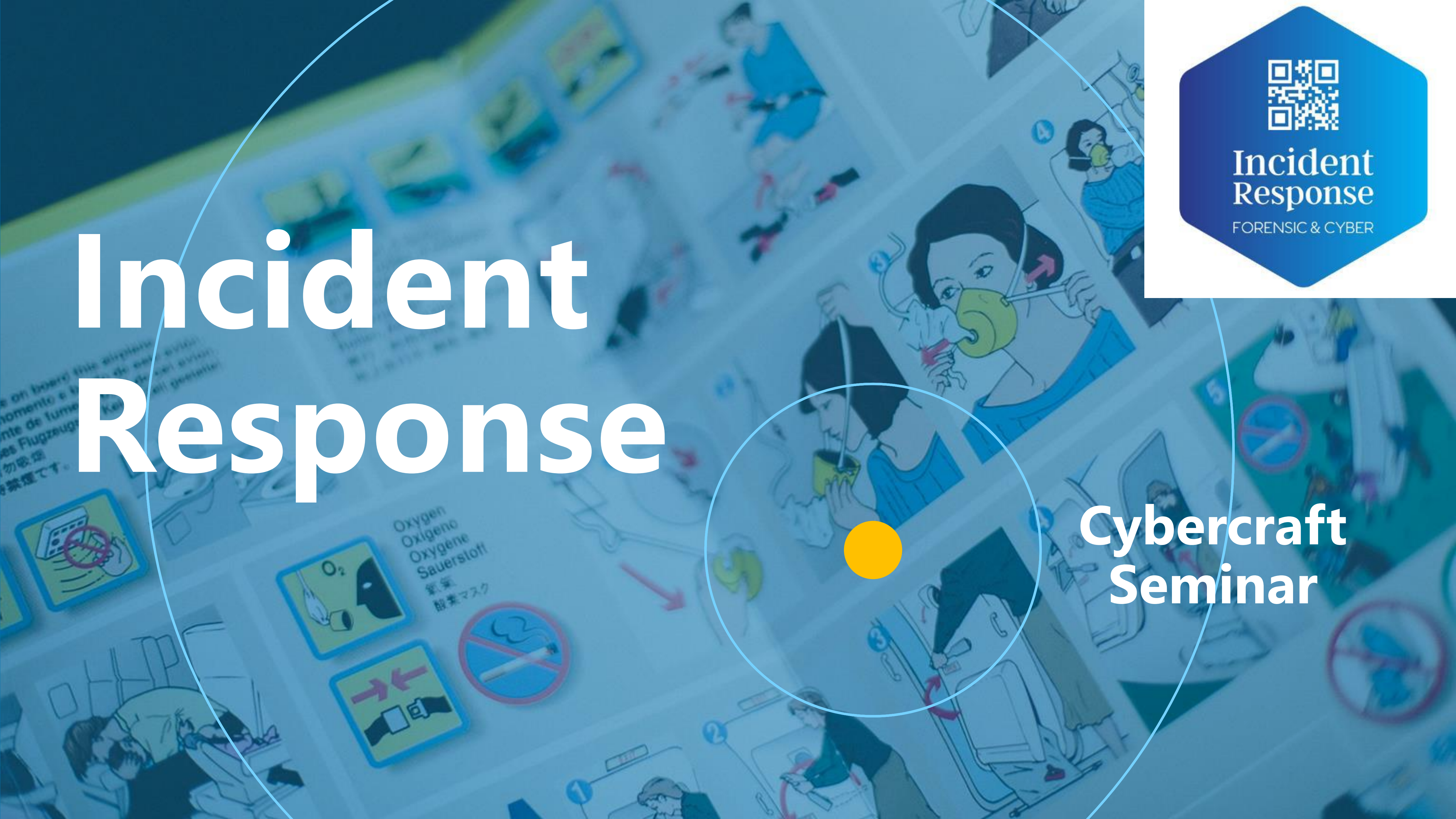


Incident Response

Cybercraft Seminar

Incident Response
FORENSIC & CYBER

INTRODUCTION

Incident Response

Our mission

To provide specialty forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Let us share some favourite tips

The purpose of this presentation is to discuss how technology is enabling organisations, whilst balancing the risks associated with Cyber.

Why Sully?

It is an intellectual hyperlink that establishes a relationship between Air Traffic Safety and Cyber Safety, and it's a great movie!

FACT

Data Breaches | WHEN, NOT IF.

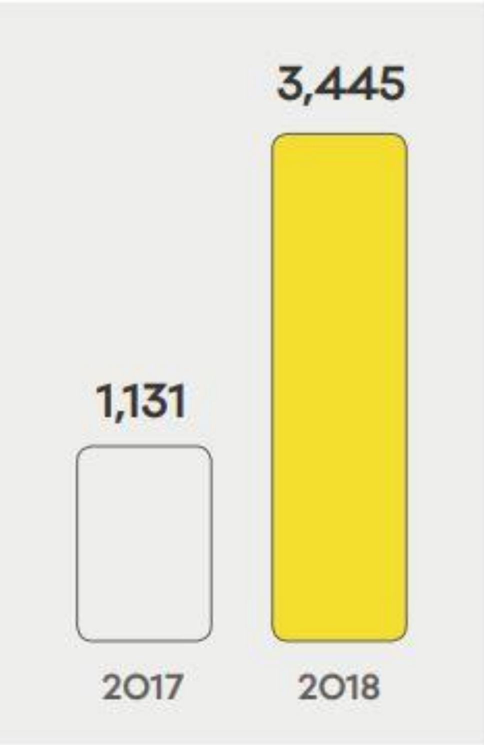
If your competitors offer more security than you, your clients may opt to entrust their data to businesses with stronger, documented cybersecurity practices

Cyber Incidents in New Zealand

Top incident categories

The **top three incident categories** for 2018 were also the highest in 2017.

Phishing and credential harvesting	1,550
Scams and fraud	1,136
Unauthorised access	303

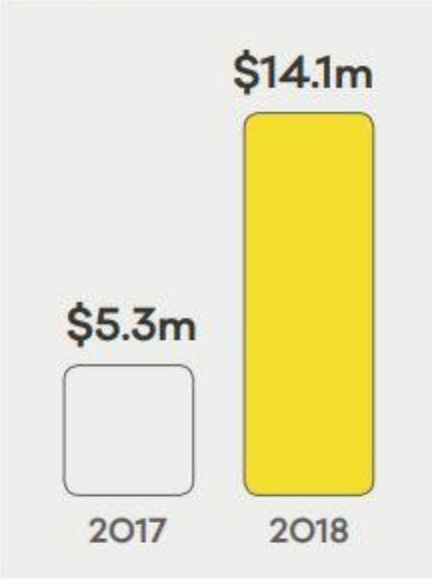


In 2018, incidents reported to CERT NZ **increased by over 200%**. These reports were received from individuals, small businesses and large organisations from all over New Zealand.

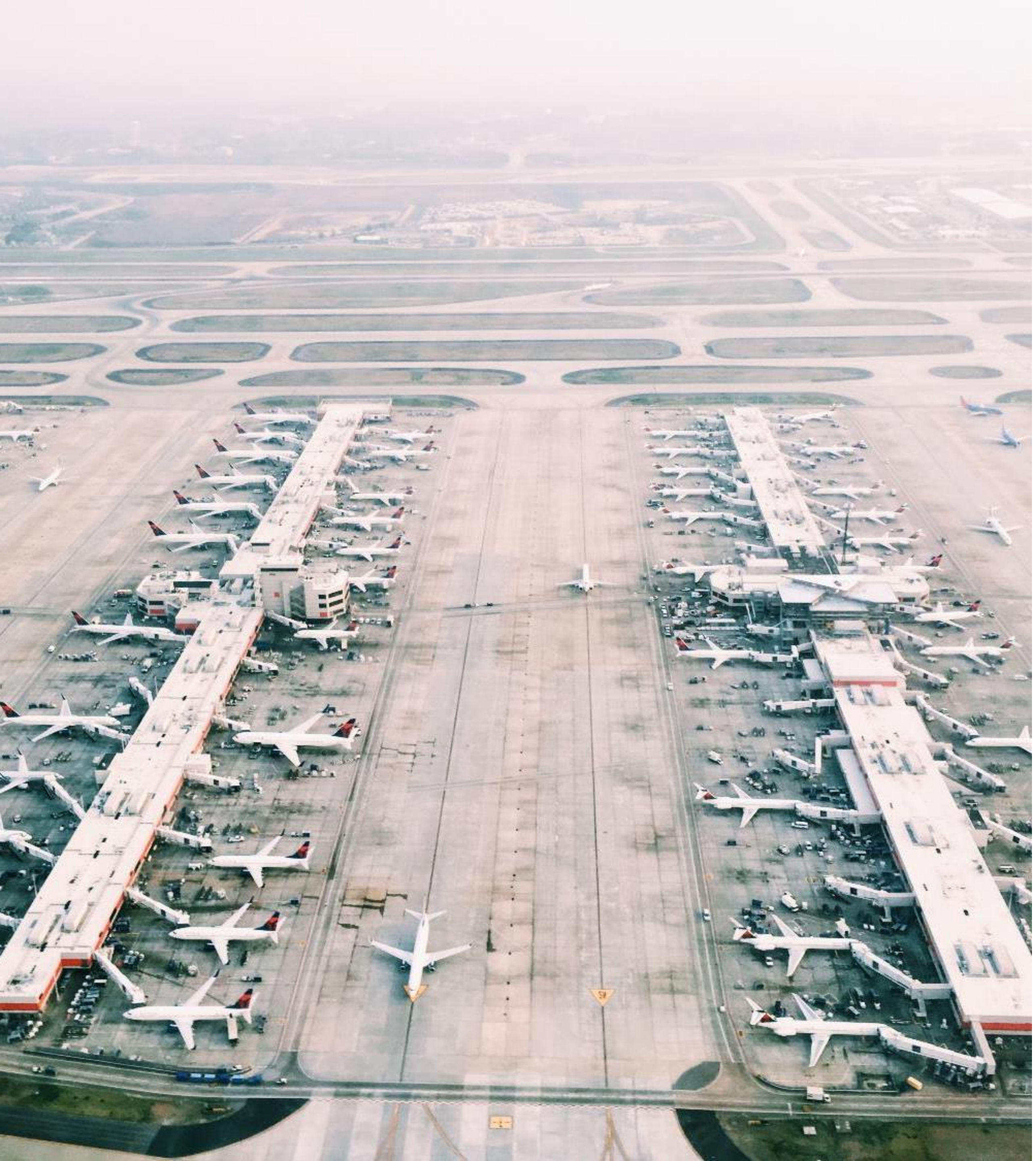
205%
increase in reports

Financial loss

18% of reports made to CERT NZ had some form of financial loss with a total value of **$14 million.**



https://www.cert.govt.nz/



1

Key Asset Identification

- **Personally Identifiable Information (PII)**
- **Intellectual property**
- **Financial and PCI details**
- **Business strategies**
- **Inventories of assets**

2

Consequences of a data security breach

- **Financial loss**
- **Reputational damage**
- **Stress on employees**
- **Possible Fines**
- **Director Accountability**

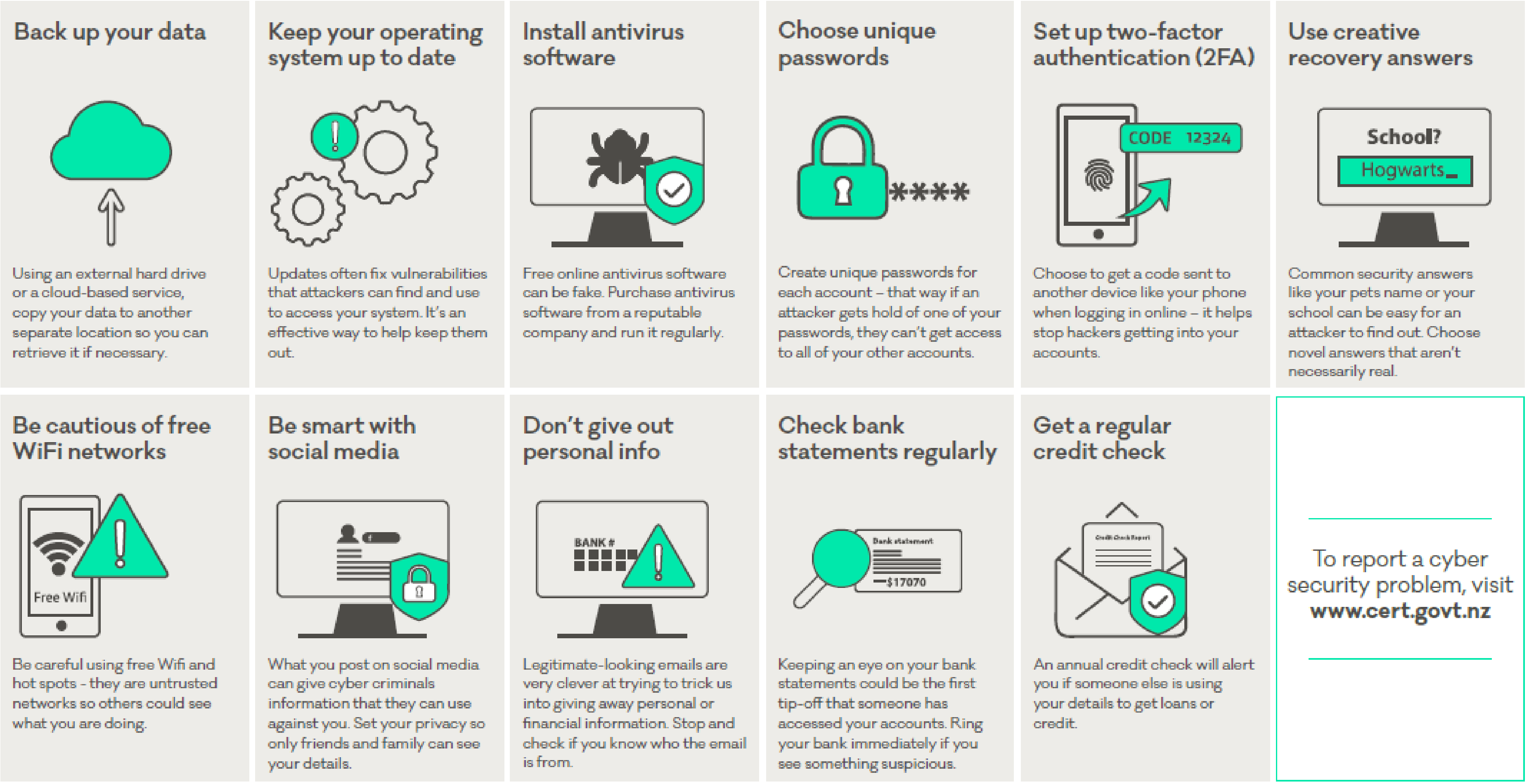
3

Basic Cyber Hygiene

- An inventory of the digital assets in the firm
- Training and awareness
- Periodic cybersecurity risk assessments
- Security strategies and controls
- A cyber incident response plan which is regularly tested
- Oversight of external business and third-party service provider arrangements
- Ongoing cyber monitoring and analysis

PREPARE

certnz Top tips for cyber security



Back up your data

Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.

Keep your operating system up to date

Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.

Install antivirus software

Free online antivirus software can be fake. Purchase antivirus software from a reputable company and run it regularly.

Choose unique passwords

Create unique passwords for each account – that way if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts.

Set up two-factor authentication (2FA)

Choose to get a code sent to another device like your phone when logging in online – it helps stop hackers getting into your accounts.

Use creative recovery answers

Common security answers like your pets name or your school can be easy for an attacker to find out. Choose novel answers that aren't necessarily real.

Be cautious of free WiFi networks

Be careful using free Wifi and hot spots - they are untrusted networks so others could see what you are doing.

Be smart with social media

What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.

Don't give out personal info

Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. Stop and check if you know who the email is from.

Check bank statements regularly

Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.

Get a regular credit check

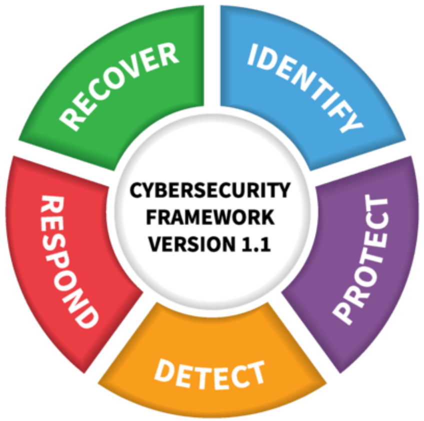
An annual credit check will alert you if someone else is using your details to get loans or credit.

To report a cyber security problem, visit **www.cert.govt.nz**

https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/

NIST Framework for Improving Critical Infrastructure Cybersecurity

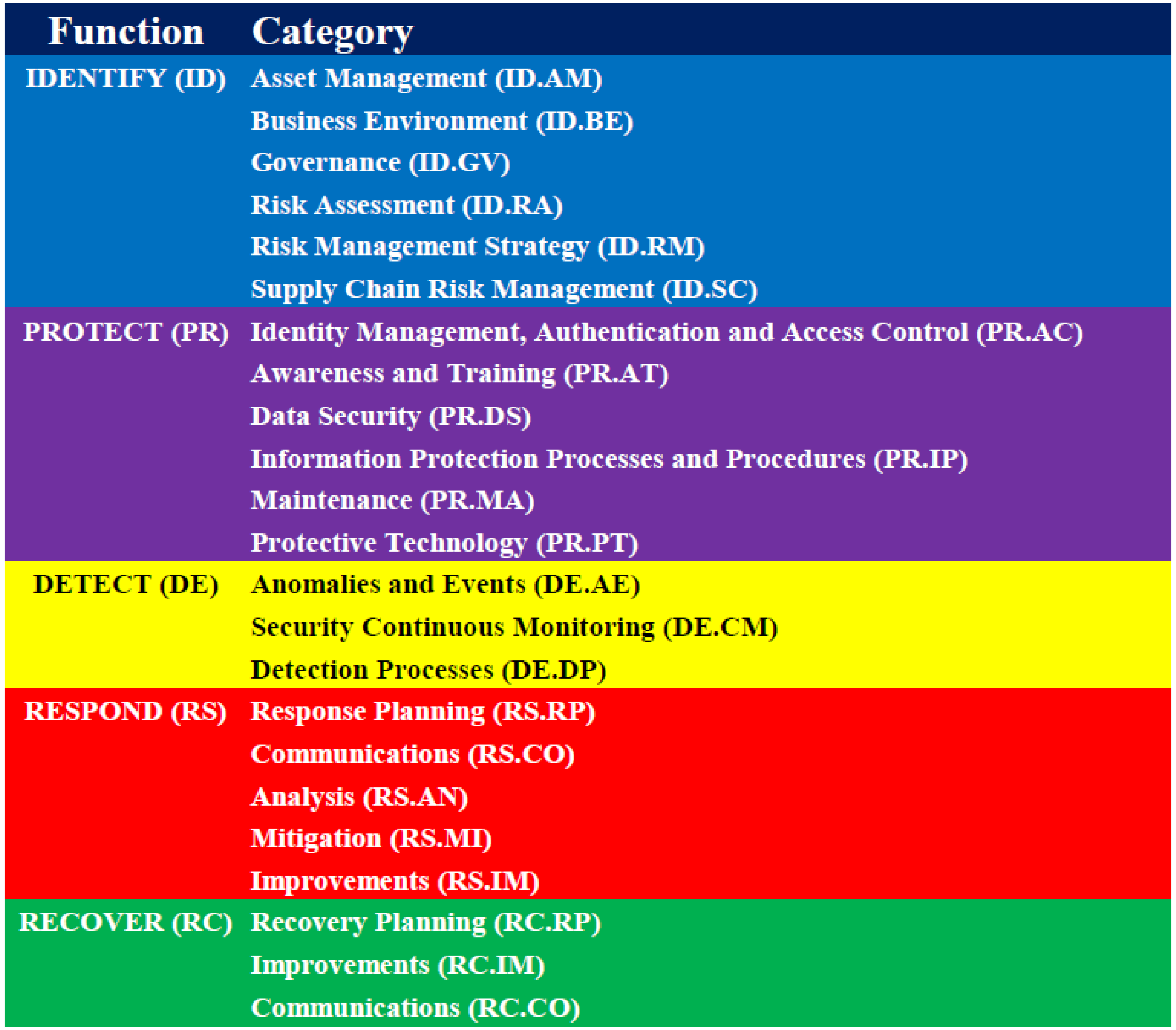
1	2	3	4	5
Identify	Protect	Detect	Respond	Recover



https://www.nist.gov/cyberframework

PREPARE

NIST Framework



Function	Category
IDENTIFY (ID)	Asset Management (ID.AM)
	Business Environment (ID.BE)
	Governance (ID.GV)
	Risk Assessment (ID.RA)
	Risk Management Strategy (ID.RM)
	Supply Chain Risk Management (ID.SC)
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)
	Awareness and Training (PR.AT)
	Data Security (PR.DS)
	Information Protection Processes and Procedures (PR.IP)
	Maintenance (PR.MA)
	Protective Technology (PR.PT)
DETECT (DE)	Anomalies and Events (DE.AE)
	Security Continuous Monitoring (DE.CM)
	Detection Processes (DE.DP)
RESPOND (RS)	Response Planning (RS.RP)
	Communications (RS.CO)
	Analysis (RS.AN)
	Mitigation (RS.MI)
	Improvements (RS.IM)
RECOVER (RC)	Recovery Planning (RC.RP)
	Improvements (RC.IM)
	Communications (RC.CO)

4

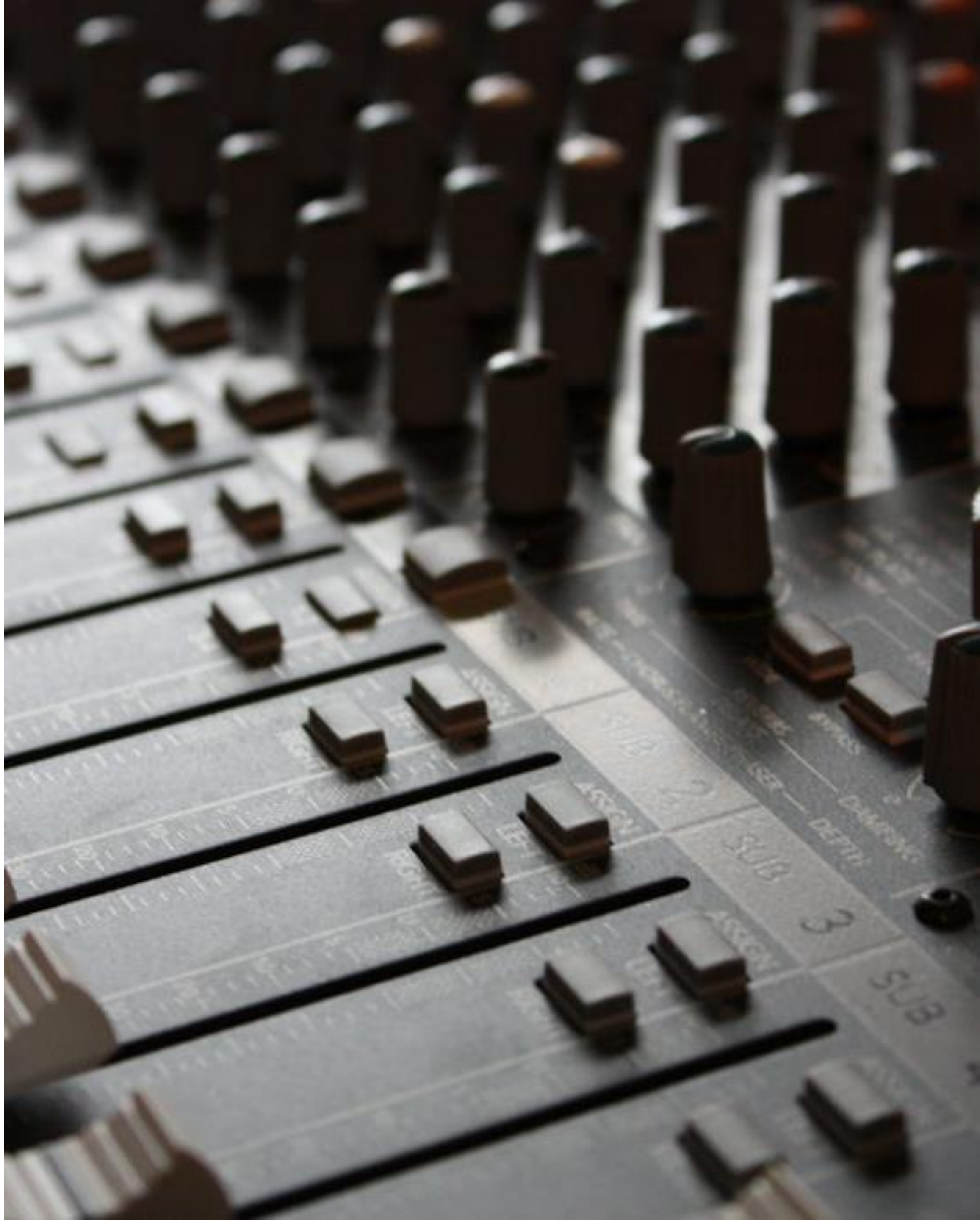
Business Continuity Plan

A business continuity plan (BCP) helps ensure that business processes can continue during a time of emergency or disaster. It is designed to immediately take effect in a disaster.

5

Disaster Recovery Plan

A documented, structured approach with instructions for responding to unplanned incidents. It is designed to ensure all aspects of a business are restored following a disaster and therefore can take longer than a BCP.



Mossack Fonesca

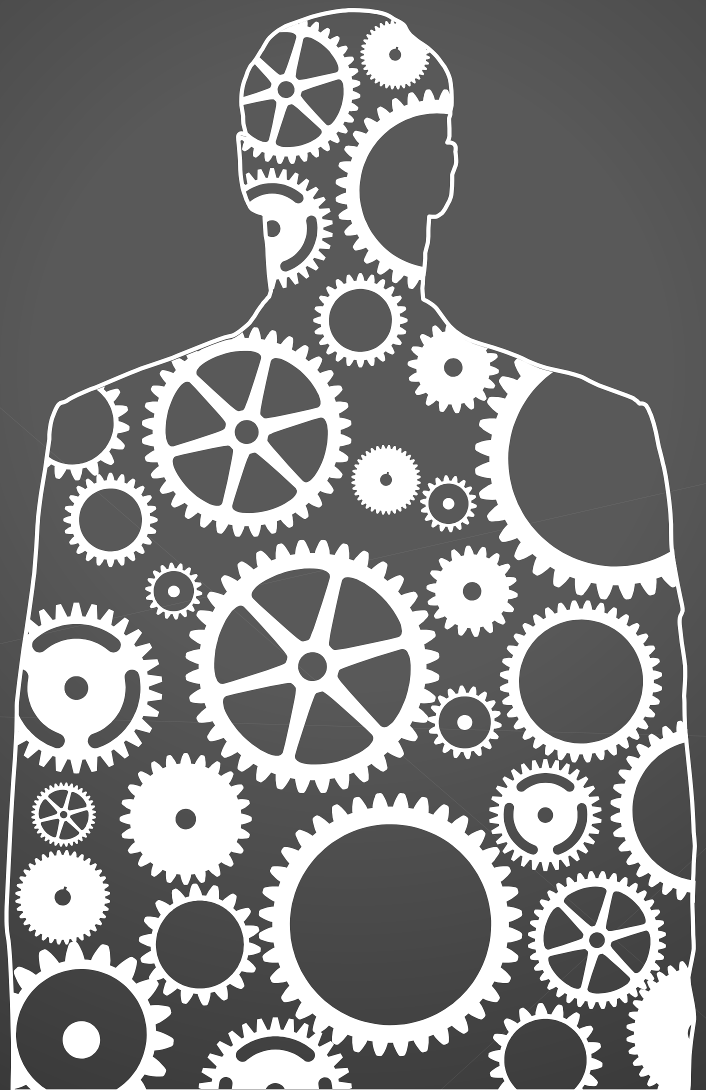
Panama Papers

150 Inquiries

2.6 Terabytes

79 Countries

Unknown Vector



11.5 million

40 Years

Biggest Leak in History

Firm Shut Down

FACT

Tabletop Exercises | PREPARE TO RESPOND.

“I've had 40 years in the air but in the end,
I'm going to be judged by 208 seconds.”
Captain Chesley Sullenberger

Tabletop Exercises

1

Scenarios

2

Injects

3

Role Play

4

Debrief

5

Improve

Tabletop Exercises Example

1

Ransomware

2

PII Data Breached

3

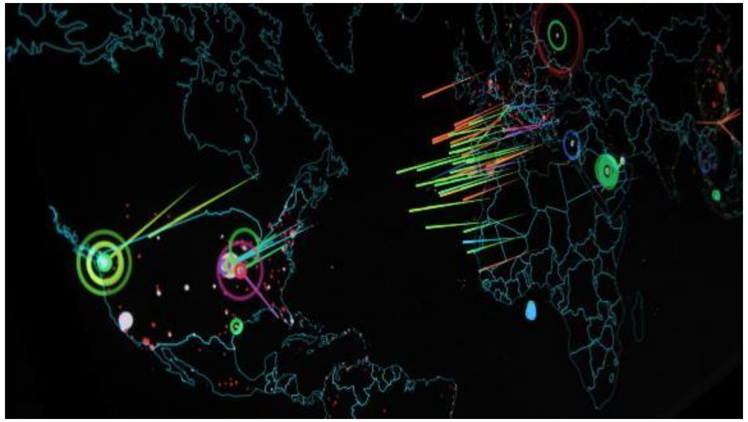
Breach Notification

4

Restoration of Systems

5

Improvements to Monitoring



PREPARE

- cyber strategy and cyber incident response plan
- test plan through simulations
- engage panel of experts (legal, forensic, PR, HR, IT)

RESPOND

- identify
- contain and eradicate

RECOVER

- carefully return to business as usual
- conduct lessons learned and update preparation

Thank you

Incident Response
FORENSIC & CYBER

Nicole Girvan
Incident Response Solutions Limited
+64 9 363 7910
+64 27 277 3549
nicole@incidentresponse.co.nz
Level 26, PwC Tower, 188 Quay St
Auckland, 1010
https://incidentresponse.co.nz